son ordinateur ou de son smartphone, elle circule sur le réseau des nœuds validateurs qui ne peuvent que l'accepter et exécuter ce qu'elle demande. L'opération est irréversible. Cette irréversibilité n'existe pas pour les virements dans le monde bancaire classique, où les établissements gardent pendant plusieurs jours la possibilité d'annuler un virement. Cette irréversibilité des transactions en cryptomonnaies est intéressante et a été généralisée avec ce qu'on dénomme des contrats intelligents, ou *smart contracts*. Ce sont des programmes qu'on dépose sur la blockchain de certaines cryptomonnaies et qui ont la capacité de détenir des unités monétaires, d'en recevoir et d'en envoyer automatiquement.

La première cryptomonnaie à offrir un langage puissant pour écrire ces *smart contracts* était ethereum (*voir «Du bitcoin à ethereum: l'ordinateur-monde»*, Pour la Science *de novembre 2016, pp. 104-109*). L'irréversibilité devient pour un *smart contract* l'impossibilité d'en arrêter le fonctionnement, qui est simultané sur chaque nœud validateur. Cela interdit de faire exécuter au programme autre chose que ce qui est prévu. Ces programmes qui, une fois définis, ne peuvent plus être arrêtés ou modifiés parce que leur fonctionnement provient du consensus d'exécution du réseau, constituent une nouveauté informatique extraordinaire. Cet ordinateur mondial, décentralisé, parfaitement fiable fait ce qu'on lui demande de faire sans que personne ne puisse l'interrompre ou le corrompre.

Cela permet par exemple de programmer des jeux d'argent et de pari où l'organisateur ne peut pas refuser de payer et ne peut partir avec la caisse quand il perd trop. Le terme d'applications décentralisées (DApp, en abrégé anglo-saxon) est souvent utilisé pour désigner ces *smart contracts*.

Grâce à ces *smart contracts*, on crée des cryptomonnaies qui ont les mêmes propriétés que celles reposant sur des blockchains spécifiques: elles sont sans autorité centrale et surveillées, indirectement maintenant, par les nœuds validateurs d'un réseau. En clair, grâce aux cryptomonnaies permettant les *smart contracts*, on définit facilement de nouvelles monnaies décentralisées sans avoir à mettre en place un réseau nouveau de nœuds validateurs.

Cette possibilité de disposer de l'équivalent d'une blockchain particulière à moindre coût en s'appuyant par exemple sur la blockchain ethereum a engendré l'apparition rapide de nouvelles cryptomonnaies, dont le nombre a explosé depuis 2016. Des cryptomonnaies liées à certaines entreprises voulant lever des fonds ont été introduites par dizaines. Les unités monétaires de ces cryptomonnaies se nomment des jetons (*tokens*) et ces opérations de >

2

LES ICO OU PRÉÉMISSIONS DE JETONS

Une ICO (pour *initial coin offering*, ou « préémission de jetons ») est une méthode de levée de fonds fondée sur une cryptomonnaie liée à l'entreprise qui veut se financer. Les jetons de la cryptomonnaie sont en général créés à l'aide d'un *smart contract (voir le texte principal)*. On peut acheter des jetons pendant la phase de démarrage de l'entreprise. Ces jetons sont cotés et échangeables sur les plateformes d'échange de cryptomonnaies. Le plus souvent le bitcoin ou l'ether sert de monnaie intermédiaire : on achète des bitcoins pour ensuite les échanger contre des jetons de l'ICO.

Les jetons de l'ICO donnent des droits particuliers concernant l'entreprise qui les a émis : droits de vote, droits d'usage des services à prix intéressants, etc. Contrairement aux actions mises en circulation lors d'une IPO (*initial public offering*, en français « introduction en Bourse »), les jetons ne représentent pas des parts de l'entreprise. Acheter les jetons d'une ICO revient à prépayer les services qui vont être proposés.

Un exemple est la société Storj Labs, à Atlanta (États-Unis), qui crée un service de stockage massif décentralisé. Les fichiers informatiques à stocker sont chiffrés et découpés en morceaux. On les copie alors – avec des redondances pour se protéger des accidents – dans la mémoire des ordinateurs acceptant de participer au réseau de stockage. La capacité du réseau dépasse 100 pétaoctets (soit 10^{17} octets), et l'objectif est d'arriver à plusieurs exaoctets (10^{18} octets). Le réseau est déjà composé de 150 000 ordinateurs capables de détenir des morceaux de fichiers confiés à Storj répartis dans 200 pays.

La société Storj Labs a levé début 2017 l'équivalent de 30 millions de dollars *via* une ICO. Leur jeton, le storjcoin, permet d'acheter de l'espace de stockage sur le réseau Storj ; il représente donc un accès privilégié aux services développés. La capitalisation des jetons Storj en février 2019, (victime de la baise générale des cours de l'année 2018) s'élevait à 18 millions de dollars. Si la société réussit, ses jetons se valoriseront.

Contrairement aux IPO, les ICO sont mal réglementées et il est considéré comme risqué de s'introduire sur ces marchés avant que des lois en assainissent et en contrôlent le fonctionnement, ce qui est en cours.